GIS\PR35-04

ADDENDUM CONTRATTUALE
per servizi erogati in modalità SaaS

Redazione	*Claudio Garna*	14/04/2026 *Data*
Verifica	Manuela Terribile	14/04/2026 *Data*
Approvazione	Andrea Tomasini	14/04/2026 *Data*

Il documento è da intendersi: **"Redatto** se provvisto del nome del redattore
"Verificato" se provvisto del nome del verificatore
"Approvato" se provvisto del nome dell'approvatore

Classificazione del documento: **Pubblico**

STORIA DELLE MODIFICHE APPORTATE

Da rev 1 a rev 2

L'addendum contrattuale è stato aggiornato con riferimento al campo di applicazione.

Da rev 2 a rev 3

Adeguato documento con riferimenti specifici alle linee guida ISO 27017 e 27018.

Da rev 3 a rev 4

Adeguato documento per implementazioni di processi.

Feinar s.r.l. con sede legale e sede operativa in Via Guido Rossa, 101 - Loc. Mier 32100 Belluno (BL), in persona del suo legale rappresentante (denominata anche "**Feinar"** o "**Fornitore"**) al fine di mettere a disposizione del **Cliente** un opportuno set informativo che consenta a quest'ultimo di usufruire della migliore esperienza possibile di servizio ed identificare prontamente le modalità di gestione di eventuali problematiche connesse direttamente o indirettamente ad esso oltre che esprimere il soddisfacimento dei requisiti richiesti in conformità con le linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2025.

Il presente addendum di applica ai servizi cloud erogati in modalità SaaS da Feinar appartenenti alla seguente lista:

- Rilevazione presenze, HR Platform (Portale azienda, Portale dipendente, BI Feinar, Scheda retributiva) e relativi Add-On di servizi correlati erogati sia tramite web app sia tramite applicazioni mobile,
- Gestione documentale (conservazione documenti e conservazione a norma),
- Gestione Fatturazione Elettronica,
- Gestione contabilità/vendite.

Quanto riportato all'interno del presente documento è da intendersi ad integrazione e migliore precisazione delle informazioni contenute nelle condizioni generali di contratto essendo un allegato allo stesso,

INFORMA

di quanto segue:

1) COLLOCAZIONE GEOGRAFICA E LUOGO DI CONSERVAZIONE DEI DATI (Rif. 6.1.3 ISO 27017 – A.12.1 ISO 27018)

Feinar ha sede legale ed operativa in Via Guido Rossa, 101 - Loc. Mier 32100 Belluno (BL). L'infrastruttura informatica necessaria alla erogazione dei servizi SaaS e dei relativi dati dedicati è collocata su server situati presso la sede del Fornitore.

Dette infrastrutture tecnologiche virtuali e reali sono nella disponibilità esclusiva di **Feinar**, che ne gestisce la configurazione e l'erogazione del servizio. Le suddette infrastrutture sono granularmente gestite dal personale Feinar che provvede ad installare, configurare e mantenere i servizi applicativi erogati. In ogni caso la conservazione dei dati avviene nell'ambito del territorio italiano ed europeo, ai fini della individuazione della legislazione applicabile in caso di controversia.

2) RUOLI E RESPONSABILITÀ (Rif. 6.1.1 ISO 27017 e 5.2 ISO 27018)

Feinar ha provveduto ad identificare specifiche responsabilità per l'erogazione dei servizi Cloud tramite la documentazione dei sistemi di gestione ISO 9001 e ISO 27001 che sono a disposizione e documentati all'interno dell'organizzazione tramite opportuni organigrammi.

I riferimenti per contatti tecnici e commerciali relativi ai servizi cloud sono i seguenti:

- Riferimento commerciali: commerciale@feinar.it
- Riferimento tecnico:
    - Piattaforma PRESENZE: hr@feinar.it, time@feinar.it, hrportal@feinar.it
    - Piattaforma DOCUMENTALE: assistenza.archiviazione@feinar.it
    - Piattaforma PORTALE DIPENDENTE: assistenza.portale@feinar.it
    - Piattaforma GESTIONALE: ass.sai@feinar.it

Feinar è impegnata ad attivare tempestivamente i servizi richiesti dal Cliente al momento della sottoscrizione delle condizioni contrattuali, che riportano la tipologia di servizi abilitati sulle proprie Piattaforme, trasmettendo tempestivamente al Cliente username e link per la generazione della password di accesso per la prima utenza di cui al successivo punto 4 del presente set informativo. Per la natura stessa dei servizi e grazie all'utilizzo della piattaforma SaaS e per le piattaforme che lo consentono, il Cliente può autonomamente attivare ulteriori utenti rispetto a quelli originariamente contrattualizzati direttamente dalla piattaforma, attraverso le proprie credenziali di autenticazione di amministratore.

Dove è previsto l'intervento in backoffice di **Feinar**, la stessa è impegnata ad attivare le nuove risorse e servizi nel più breve tempo possibile, compatibilmente con la tipologia dell'intervento. Nessuna responsabilità potrà comunque essere ascritta al Fornitore per il caso di ritardo nell'attivazione del servizio; la richiesta di chiarimenti o la segnalazione di eventuali problematiche, da eseguire utilizzando la messaggistica elettronica.

È facoltà del Cliente chiedere a **Feinar**, mediante comunicazione inviata tramite e-mail, la messa a disposizione di risorse o servizi aggiuntivi rispetto a quelli già attivati. In tal caso alla richiesta inoltrata dal Cliente farà seguito da parte di **Feinar**, secondo le tempistiche concordate con il cliente, la redazione di un preventivo specifico in base alla disponibilità delle risorse o dei servizi richiesti. Il momento perfezionativo dell'accordo dove in questo caso intendersi identificato nella conferma da parte del Cliente dell'accettazione del preventivo ricevuto, da cui decorre anche il termine per l'attivazione delle risorse o dei servizi contrattualizzati previsto dal precedente capoverso.

Il presente Addendum adotta un modello di responsabilità condivisa per la sicurezza del servizio Cloud, in conformità con le linee guida ISO/IEC 27017. La seguente matrice definisce la ripartizione delle responsabilità tra Feinar (il Fornitore) e il Cliente per i principali domini di sicurezza.

Dominio di Sicurezza	Responsabilità di Feinar	Responsabilità del Cliente	Responsabilità Condivisa
Infrastruttura Fisica e di Rete	Gestione e sicurezza dei data center, dell'hardware fisico (server, storage, apparati di rete) e della connettività di base.	N/A	
Infrastruttura di Virtualizzazione	Gestione, configurazione e hardening dell'hypervisor e dei componenti di virtualizzazione per garantire la segregazione degli ambienti.	N/A	
Sistema Operativo e Middleware	Installazione, patching, hardening e monitoraggio dei sistemi operativi e del middleware (es. web server, database) su cui si basa l'applicazione SaaS.	N/A	
Applicazione SaaS	Sviluppo sicuro, manutenzione, aggiornamento e monitoraggio della sicurezza dell'applicazione (es. Rilevazione Presenze, HR Platform).	Configurazione delle funzionalità applicative messe a disposizione (es. parametri, workflow).	
Gestione Identità e Accessi (IAM)	Fornitura della piattaforma per la gestione degli accessi e abilitazione delle utenze iniziali.	Gestione del ciclo di vita delle utenze (creazione, modifica, disabilitazione), revisione periodica dei permessi, gestione delle credenziali (password complexity, rotazione, non divulgazione).	X
Dati del Cliente	Protezione dei dati a riposo e in transito, implementazione delle policy di backup e disaster recovery, gestione della cancellazione sicura a fine contratto.	Classificazione dei dati inseriti, gestione della liceità del trattamento, adempimenti normativi specifici relativi ai propri dati.	X
Sicurezza degli Endpoint	N/A	Protezione dei dispositivi (PC, smartphone, tablet) utilizzati per accedere al servizio Cloud (es. antivirus, firewall, crittografia locale).	
Monitoraggio e Risposta agli Incidenti	Monitoraggio dell'infrastruttura e delle applicazioni per rilevare e rispondere a incidenti di sicurezza. Notifica al Cliente in caso di violazione dei dati.	Monitoraggio delle attività dei propri utenti e segnalazione a Feinar di comportamenti anomali.	X

3) Definizione, Ripartizione e Modifica delle Responsabilità di Sicurezza (Rif. 8.1.1, 8.2.2 ISO 27017)

In conformità con le migliori pratiche per i servizi cloud, le Parti riconoscono che la sicurezza delle informazioni è una responsabilità condivisa. Le responsabilità relative alla sicurezza del servizio, dei dati e delle infrastrutture sono definite e ripartite tra **Feinar** (il Fornitore) e il Cliente come dettagliato nel "Modello di Responsabilità Condivisa" di cui all'Articolo 2 del presente Addendum. Tale modello costituisce parte integrante del presente accordo e definisce in modo puntuale gli obblighi di ciascuna Parte per i diversi domini di sicurezza, inclusi ma non limitati a: infrastruttura fisica e di rete, virtualizzazione, sistema operativo, applicazione, gestione delle identità e degli accessi, protezione dei dati e monitoraggio.

Qualsiasi modifica ai servizi cloud forniti, che abbia un impatto sulle responsabilità di sicurezza definite nel presente Addendum o sulle misure di sicurezza implementate da **Feinar**, sarà gestita attraverso un processo formale di change management. **Feinar** si impegna a notificare al Cliente, con un preavviso di almeno 60 giorni, qualsiasi modifica pianificata che possa influire in modo sostanziale sulla postura di sicurezza del servizio o sugli obblighi del Cliente. La notifica includerà una descrizione della modifica, le sue implicazioni per la sicurezza e le eventuali azioni richieste al Cliente. Le modifiche che comportano una variazione delle presenti pattuizioni contrattuali saranno formalizzate tramite un'appendice scritta e controfirmata da entrambe le Parti.

4) CRITERI DI AUTENTICAZIONE (Rif. 9.2.1-9.2.2-9.2.3-9.2.4,9.4.1, 9.4.4 ISO 27017 e 5.16 – 5.17 ISO 27018)

All'attivazione del servizio, vengono definite le integrazioni con i sistemi cliente per l'autenticazione e l'autorizzazione delle utenze, **Feinar** configura e abilita le utenze che vengono comunicate al cliente per l'accesso **al servizio stesso.**

È cura di Feinar o del Cliente stesso in qualità di amministratore e per le piattaforme che lo consentono, comunicare agli utenti finali le relative credenziali che saranno comunque da cambiare al primo accesso della piattaforma.

La password inserita dovrà prevedere criteri di password complexity.

L'onere di provvedere alla regolare modifica della password di accesso viene assunto dal Cliente; lo stesso per la conservazione delle credenziali di accesso e della non divulgazione di esse anche ai fini della prevenzione di accessi non autorizzati. Fatto salvo quanto specificato in caso di crittografia dei dati, **Feinar** si impegna a prestare assistenza al Cliente – ove necessario – per eventuali modifiche delle credenziali di accesso ovvero recupero delle stesse in caso di smarrimento. Eventuali richieste di supporto tecnico o reset della password dovranno essere effettuate a Feinar tramite e-mail o direttamente al Cliente, per le piattaforme che lo consentono, attraverso i canali da esso autorizzati. A tutela della sicurezza dei dati e delle infrastrutture, **Feinar** accetterà le richieste solo se provenienti dal referente del servizio o autorità riconosciuta (es: resp. Acquisti o responsabile dei servizi IT) e si riserva di richiedere l'esibizione di dati che consentano l'identificazione del richiedente o comunque la conferma della provenienza della richiesta dall'avente diritto, ed in ogni caso di verificare con qualunque mezzo l'effettivo potere di quest'ultimo.

Le piattaforme permettono una profilazione granulare delle utenze che sono configurabili Feinar o dal Cliente, per le piattaforme che lo consentono. Alle utenze verranno associati successivamente i Ruoli organizzativi assegnati.

Tramite l'analisi dei log, è possibile visualizzare gli accessi effettuati dove risultano anche gli accessi negati permettendo una analisi di potenziali account compromessi.

La gestione del ciclo di vita delle utenze, inclusa la creazione, la modifica dei ruoli autorizzativi e la disabilitazione tempestiva degli account in caso di cessazione del rapporto di lavoro resta sempre in capo

a **Feinar**. **Feinar** o il Cliente, per le piattaforme che lo consentono, gestisce le credenziali ed o permessi di accesso. Il Cliente è responsabile del corretto e puntuale utilizzo delle credenziali. **Feinar**, inoltre, implementa controlli per la disabilitazione automatica di utenze inattive per un periodo superiore a 90 giorni, previa notifica all'amministratore del Cliente. La revisione periodica degli accessi, a carico di **Feinar**, essendo una responsabilità condivisa su richiesta potrà essere fornita al Cliente sotto forma di report di controllo.

5) CRITTOGRAFIA (Rif. 10.1, 18.1.5 ISO 27017 e 8.24 ISO 27018)

Feinar garantisce la protezione dei dati del Cliente attraverso l'adozione di misure di crittografia standard. I dati in transito tra il dispositivo del Cliente e i server di **Feinar** sono protetti tramite protocolli crittografici robusti (es. TLS 1.2 o superiore). I dati a riposo (dati memorizzati sui dischi e nei backup) sono protetti tramite crittografia a livello di volume o di database. La gestione delle chiavi di crittografia è di esclusiva competenza di **Feinar**, che ne garantisce la protezione e il ciclo di vita secondo procedure interne formalizzate. Eventuali requisiti di crittografia aggiuntivi o specifici possono essere concordati tramite accordo separato.

Dovrà inoltre considerarsi a carico esclusivo del Cliente la verifica della compliance della tipologia di crittografia sviluppata o richiesta alla normativa nazionale di riferimento per competenza o materia, dipendendo tali informazioni dalla tipologia di attività svolta dal Cliente, dalla natura dei dati trattati e dalle finalità sottese al trattamento dei medesimi.

6) MODIFICHE AL SERVIZIO (Rif. 12.1.2 ISO 27017)

Per garantire la migliore esperienza dei servizi offerti e consentire al Cliente il monitoraggio delle condizioni di erogazione dei servizi, **Feinar** è impegnata a rendere nota la versione applicativa dei servizi Cloud erogati direttamente attraverso l'interfaccia utilizzata dal Cliente.

Il *versioning* applicativo viene diffuso, in base alle necessità, con comunicazione mirata ai Clienti attraverso l'aggiornamento dell'UDI del software da cui si può risalire agli aggiornamenti e/o alle modifiche dell'infrastruttura o delle piattaforme, previa verifica che tali non possano comportare alcun prevedibile effetto negativo relativamente all'erogazione del servizio. La pubblicazione di dette informazioni, poiché relative a interventi che non costituiscono prevedibilmente alcun rischio per il servizio o per il Cliente, costituisce principio di trasparenza da parte di **Feinar**, pur in assenza di ogni obbligo contrattuale al riguardo.

Feinar è altresì impegnata nel comunicare al Cliente, mediante trasmissione di comunicazione diretta, l'effettuazione di modifiche hardware o software che abbiano il prevedibile effetto di incidere sulla disponibilità e qualità dei servizi e sulla sicurezza delle informazioni e dei dati del Cliente. Fatto salvo il caso di causa sopravvenuta ed imprevedibile o forza maggiore, tutte le modifiche programmate all'infrastruttura che si rendano necessarie per la prosecuzione o il miglioramento del servizio e che abbiano il prevedibile effetto di incidere sulla qualità dei servizi, saranno comunicate al Cliente e con lo stesso, viene definita la data di aggiornamento dei servizi. All'atto della comunicazione, sarà indicato da **Feinar** il tipo di intervento da effettuare, la prevedibile durata di esso, i prevedibili effetti sul servizio e/o eventuali situazioni di rischio per i dati del Cliente. Nel tempo di preavviso stabilito, il Cliente potrà sempre richiedere chiarimenti e/o precisazioni mediante i contatti riportati sopra o comunque tramite e-mail (vedi punto 2).

Nel caso di modifiche che dovessero rendersi necessarie per effetto di atti, fatti o comunque eventi non prevedibili, tali da determinare un'urgenza, **Feinar** è impegnata a svolgere tutte le attività di modifica con le modalità tecniche che siano ritenute le migliori disponibili per la garanzia di qualità del servizio e la sicurezza dei dati di proprietà del Cliente; in tali circostanze, **Feinar** si impegna a comunicare al Cliente l'avvio delle operazioni e lo stato di avanzamento delle stesse.

Al termine di ogni modifica o implementazione che ha un impatto sul *versioning*, sia essa pianificata o improvvisa, **Feinar** provvederà all'invio di una comunicazione al Cliente attestante l'avvenuto completamento delle operazioni ed il relativo esito.

7) BACKUP (Rif. 12.3.1 ISO 27017 e 8.13 ISO 27018)

Feinar gestisce le policy di backup dei dati dei servizi Cloud erogati ai Clienti secondo le policy descritte all'interno della:

- Procedura di backup dei servizi cloud

È altresì facoltà del Cliente, all'atto della stipula del contratto o successivamente ad essa, chiedere la predisposizione a cura di **Feinar** di servizi di backup ulteriori rispetto a quelli disponibili all'interno della piattaforma, sia interni che esterni ad essa. In tal caso, seguirà all'eventuale richiesta del Cliente la predisposizione da parte di **Feinar** di un relativo preventivo.

8) SINCRONIZZAZIONE OROLOGI DI SISTEMA (Rif. 12.4.4 ISO 27017)

Per la determinazione dell'orario dei servizi Cloud offerti, **Feinar** utilizza di norma l'ora fornita da Server di dominio. Non è possibile accettare richieste di personalizzazione delle configurazioni su specifica del Cliente, in quanto tali configurazioni sono applicate all'intera infrastruttura gestita da **Feinar.**

9) INFORMAZIONI RELATIVE ALLA SICUREZZA NELLE FASI OPERATIVE E DI SVILUPPO (Rif. 14.2.1 ISO 27017 – 5.14 ISO 27018)

Feinar è impegnata nel mettere a conoscenza del Cliente la tipologia dei servizi di sicurezza utilizzati per la tutela dei dati trattati attraverso l'infrastruttura in Cloud, o di concordare con il Cliente – dietro pagamento di un corrispettivo per la personalizzazione – l'installazione, l'implementazione o comunque l'utilizzo di maggiori livelli di sicurezza. **Feinar** si impegna a mettere a disposizione unicamente le conoscenze e gli elementi che sono indispensabili al Cliente per ottenere la migliore esperienza d'uso dei servizi contrattualizzati, rimanendo peraltro facoltà di **Feinar** di non divulgare elementi dei sistemi di sicurezza che per tipologia o per caratteristiche oggettive possano essere suscettibili di un uso malevolo da parte di eventuali terzi soggetti, con rischio per la sicurezza dei dati e/o per l'infrastruttura.

Salvo sia diversamente disposto nel Contratto o in eventuali pattuizioni aggiuntive, **Feinar** utilizza di norma sistemi di sicurezza della rete (es. firewall), sicurezza dei sistemi (es. monitoraggio dell'uso delle risorse) e sicurezza gestionale (es. applicazione di patch correttive e di sicurezza) per la protezione dell'infrastruttura da utilizzi impropri o prevedibili rischi di sicurezza, essendo riconducibili a **Feinar** le responsabilità relative al funzionamento delle piattaforme SaaS, con garanzia della disponibilità dei servizi al Cliente con le caratteristiche e le risorse contrattualizzate.

Nel caso di nuovi sviluppi o aggiornamento degli applicativi propri e/o di terze parti, **Feinar** è impegnata a rispettare una politica di sviluppo sicuro mediate effettuazione dei test di funzionamento in ambienti di sviluppo separati rispetto a quelli in cui viene garantita l'operatività del servizio, al fine della individuazione di eventuali bug o malfunzionamenti prima della messa in esercizio degli applicativi nella versione aggiornata, il tutto in osservanza degli standard internazionali in materia di procedure di sviluppo sicuro.

Periodicamente è prevista una scansione con tool di analisi delle vulnerabilità al fine di effettuare i dovuti aggiornamenti dell'infrastruttura a fronte delle vulnerabilità identificate.

Salvo esplicita richiesta del Cliente, **Feinar** non utilizza supporti fisici esterni per il trasferimento dei dati, preferendo per ragioni di sicurezza e tracciabilità trasferimenti esclusivamente virtuali. In caso di utilizzo di supporti fisici saranno concordate con il Cliente le tipologie di supporto, le modalità di utilizzo degli stessi e gli elementi atti a garantire la sicurezza dei dati del Cliente e dell'infrastruttura di proprietà di **Feinar,** utilizzata per l'erogazione dei servizi Cloud.

10) PEER CLOUD SERVICES e SUBFORNITORI (Rif. 15.1 ISO 27017)

Per l'erogazione dei servizi cloud **Feinar** si avvale dell'intervento di subfornitori certificati per il trattamento di dati, che anche se conservati all'esterno del perimetro dell'infrastruttura tecnologica sono direttamente riconducibili alla proprietà ed al controllo di **Feinar**.

11) RACCOLTA DELLE EVIDENZE (Rif. 16.1 ISO 27017 – 5.28, A10.1 ISO 27018)

Qualora si evidenzino elementi che consentano di ritenere fondato il timore di esposizione dei dati a rischi o incidenti, **Feinar** è impegnata a mettere a disposizione del Cliente la propria collaborazione per l'accertamento dell'esistenza o meno di vulnerabilità, con successiva analisi delle cause.

Nel contratto dei servizi Cloud SaaS è indicato il responsabile del trattamento dei dati personali fornito dal Cliente a **Feinar** che è responsabile di attuare gli accordi e le istruzioni definiti nel contratto.

Qualora un Cliente possa anche solo sospettare di una vulnerabilità o una perdita di riservatezza, integrità e disponibilità di dati ed informazioni dei servizi Cloud, provvederà a contattare il supporto tecnico di **Feinar**. Sarà cura di **Feinar** prendere in carico tali ticket con una coda di priorità atta a garantire una risposta congrua con i tempi previsti legislativamente per le comunicazioni agli enti preposti che dovrà effettuare con il Cliente (es: 72 ore nel caso di Data Breach).

Nel caso in cui sia **Feinar** ad avere certezza o anche solo il sospetto del concretizzarsi di un evento che possa avere un impatto sulla riservatezza, integrità o disponibilità dei dati, **Feinar** si impegna a comunicare tali circostanze al Cliente non appena venuta a conoscenza dell'evento e comunque entro 72 ore dalla conoscenza avutane, mediante invio di e-mail all'indirizzo di contatto indicato nel contratto.

12) PROTEZIONE DEI DATI (Rif. 18.1 ISO 27017 – A2, A3, A6, A11.1 ISO 27018)

Per quanto concerne la protezione dei dati, **Feinar** è impegnata a rispettare la legislazione italiana in materia, ivi espressamente comprese le norme derivanti dai regolamenti europei e/o direttive direttamente applicabili, tra le quali il Regolamento UE n. 679/2016 "GDPR". In tutti i casi **Feinar** si impegna a garantire gli standard per la sicurezza dei dati previsti da ACN – Agenzia per la Cybersecurity Nazionale e le best practices di volta in volta indicate dal CSIRT Italiano. Nell'ambito dell'attività aziendale tutto il personale coinvolto nelle attività è vincolato alla riservatezza con riferimento a tutte le informazioni apprese o trattate nell'esercizio delle proprie mansioni, come previsto dai regolamenti interni. A richiesta del Cliente, **Feinar** è disponibile a fornire al Cliente tutte le informazioni relative agli accorgimenti utilizzati per la tutela dei dati, previa sottoscrizione da parte del Cliente di impegno alla riservatezza e con la sola esclusione di elementi di dettaglio la cui divulgazione possa a sua volta costituire pericolo per la sicurezza dei dati o delle infrastrutture.

Salvo espressa e specifica autorizzazione del Cliente, da rilasciarsi alla stipula del contratto o mediante profilazione dell'utente nell'ambito della piattaforma, i dati trattati da **Feinar** saranno utilizzati da quest'ultima ai fini del corretto e tempestivo adempimento delle obbligazioni contrattuali e della gestione tecnica ed amministrativa del rapporto inerente i servizi resi; **Feinar** è impegnata a verificare che anche i subfornitori e comunque tutti i soggetti che vengano a conoscenza di tali dati nell'ambito della normale gestione del contratto, adottino le medesime limitazioni all'uso dei dati raccolti.

Tutte le richieste di informazioni relative al trattamento dei dati e/o agli elementi di sicurezza utilizzati per la loro conservazione possono essere inoltrate dal Cliente all'indirizzo e-mail gdpr@feinar.it da intendersi quale punto di contatto del titolare del trattamento del dato. Le informazioni relative agli elementi di sicurezza utilizzati per la conservazione dei dati saranno comunicate unicamente laddove la conoscenza di essi da parte dei richiedenti non determini l'insorgenza di rischi per la detenzione e la sicurezza dei dati medesimi.

Feinar, inoltre, agisce come Responsabile del trattamento dei dati personali per conto del Cliente. In tale ruolo, **Feinar** si impegna a:

- Limitazione delle finalità (Rif. A.2): Trattare i dati personali del Cliente esclusivamente per le finalità connesse all'erogazione e al miglioramento dei servizi contrattualizzati, senza utilizzarli per finalità proprie, di marketing o di profilazione pubblicitaria.
- Limitazioni d'uso, cancellazione e restituzione (Rif. A.3): Alla cessazione del rapporto contrattuale, restituire e/o cancellare in modo sicuro tutti i dati personali.
- Obblighi di comunicazione (Rif. A.6): Informare tempestivamente il Cliente di qualsiasi richiesta legalmente vincolante di divulgazione dei dati personali da parte di un'autorità, a meno che la legge non lo vieti.
- Obblighi di riservatezza (Rif. A.11.1): Garantire che tutto il personale autorizzato ad accedere ai dati personali sia contrattualmente vincolato a obblighi di riservatezza.

13) CONSERVAZIONE DEI LOG (Rif. 12.4, 7.2.2, 8.1.1, 16.1 ISO 27017 – 8.15 ISO 27018)

Feinar detiene direttamente informazioni dei LOG relativi alle piattaforme e alle macchine virtuali delle istanze dei servizi dei Clienti e dei dati da esse derivati (Backup, agenti installati sui server, etc..) essendo gli stessi gestiti direttamente ed unicamente da **Feinar.**

Feinar implementa un sistema di logging centralizzato che registra gli eventi rilevanti per la sicurezza a livello di infrastruttura, sistema operativo e applicazione (Rif. 12.4.1 ISO 27001). I log relativi alle attività degli utenti del Cliente sono presenti all'interno dell'applicazione. Su richiesta motivata, legata a indagini su incidenti di sicurezza o a requisiti di conformità, **Feinar** fornirà al Cliente estratti di log infrastrutturali pertinenti, garantendo al contempo, tramite procedure di anonimizzazione o mascheramento, la non esposizione di informazioni relative ad altri clienti. Tale attività di supporto è inclusa nei servizi base, salvo richieste di analisi complesse e continuative che saranno oggetto di valutazione separata.

Al termine del rapporto contrattuale, e fatti salvi i diritti previsti per il Cliente dal GDPR, **Feinar** è impegnata a mantenere i requisiti definiti nel punto 14.

14) VERIFICA DEGLI STANDARD DI SICUREZZA E AUDIT (Rif. 14.1, 18.2.1 ISO 27017 – 5.35 ISO 27018)

Feinar dimostra la propria conformità tramite certificazioni di terze parti (es. ISO/IEC 27001, 27017, 27018), i cui certificati e report di sintesi sono messi a disposizione del Cliente. Il Cliente ha il diritto di verificare la conformità di Feinar agli obblighi contrattuali.

Tale diritto può essere esercitato tramite:

a) La revisione della documentazione di sicurezza e dei report di audit di terze parti forniti da **Feinar**;

b) La facoltà di richiedere, con un preavviso ragionevole e non più di una volta all'anno, un audit di seconda parte. L'audit sarà condotto da un revisore qualificato e indipendente, concordato tra le Parti e vincolato da un accordo di riservatezza. L'ambito dell'audit sarà limitato ai servizi e ai dati del Cliente. I costi diretti dell'audit saranno a carico del Cliente, mentre **Feinar** garantirà la collaborazione del proprio personale per un tempo ragionevole senza costi aggiuntivi. Feinar non potrà negare irragionevolmente l'accesso a informazioni o luoghi pertinenti, fermo restando il diritto di proteggere i dati di altri clienti e i propri segreti commerciali.

15) RIMOZIONE DEI DATI IN CASO DI CESSAZIONE DEL RAPPORTO (Rif. CLD 8.1.5 ISO 27017 – A10.3 ISO 27018)

Al termine del rapporto contrattuale per l'utilizzo dei servizi Cloud erogati, **Feinar** ed il Cliente concorderanno come e se procedere con l'esportazione e/o alla cancellazione di tutti i dati in qualunque

forma presenti sulla piattaforma a sé riconducibili. La cancellazione dei dati dovrà essere effettuata a cura della Feinar. Una volta eliminati, **Feinar** non sarà in alcun modo responsabile della perdita di eventuali dati del Cliente.

16) TUTELA DEL DIRITTO D'AUTORE E COPYRIGHT. (Rif. 18.1.2 ISO 27017)

L'Organizzazione rispetta la normativa sui diritti di proprietà intellettuale mettendo a disposizione dei clienti dei canali di comunicazione dedicati. Qualora il cliente abbia necessità di porre qualsiasi domanda, approfondire la gestione del diritto d'autore e del copyright o anche aprire una segnalazione inerente alla tematica potrà contattare il Fornitore all'indirizzo PEC: feinar@legalmail.it.

17) SEPARAZIONE DEGLI AMBIENTI DI VIRTUALIZZAZIONE DEI CLIENTI (CLD 9.5.1 ISO 27017)

Gli ambienti dei servizi SaaS sono progettati e gestiti in modalità multi-tenant, garantendo per ciascun cliente la segregazione logica e l'isolamento dei dati e delle risorse.

18) Hardening e Gestione Vulnerabilità (Rif. CLD 9.5.2, 12.1.3, 18.1.3 ISO 27017)

Feinar adotta procedure di hardening per i sistemi operativi e le macchine virtuali (Rif. CLD 9.5.2 ISO 27017) basate su benchmark di sicurezza riconosciuti, al fine di ridurre la superficie di attacco. Viene inoltre implementato un processo di gestione delle vulnerabilità che include scansioni periodiche e l'applicazione tempestiva delle patch di sicurezza. **Feinar** monitora costantemente la capacità e le performance dell'infrastruttura (Rif. 12.1.3 ISO 27017) per garantire la continuità e la qualità del servizio.

19) Monitoraggio del Servizio (Rif. CLD 12.1.5, CLD 12.4.5)

Feinar implementa un sistema di monitoraggio continuo sull'utilizzo delle risorse dell'infrastruttura cloud (es. CPU, RAM, storage, larghezza di banda) per garantire che la capacità sia adeguata a soddisfare i livelli di servizio concordati. **Feinar** si impegna a pianificare e ad adeguare proattivamente la capacità delle risorse per prevenire il degrado delle prestazioni.

a. Accesso ai Log Applicativi: tramite le funzionalità di reporting della piattaforma è possibile accedere ai log relativi alle attività svolte dagli utenti all'interno dell'applicazione (es. accessi, operazioni principali).

b. Fornitura di Log di Sistema: **Feinar** raccoglie e conserva in modo sicuro i log di sistema e di sicurezza (es. log di firewall, accessi amministrativi, eventi del sistema operativo) per un periodo non inferiore a 6 mesi, in conformità con le normative vigenti e le policy interne. Tali log sono protetti per garantirne l'integrità e l'inalterabilità.

c. Diritto di Accesso ai Log: In caso di incidente di sicurezza o per specifiche e documentate esigenze di conformità, il Cliente ha il diritto di richiedere a **Feinar** l'accesso a estratti dei log di sistema e di sicurezza pertinenti alle proprie istanze di servizio. **Feinar** fornirà tali informazioni entro un tempo ragionevole, assicurando che i dati relativi ad altri clienti siano opportunamente mascherati o rimossi per proteggerne la riservatezza. Tale diritto di accesso è parte integrante del servizio fornito e non è subordinato, per richieste ragionevoli e non continuative, ad accordi contrattuali aggiuntivi. Questo è in linea con il diritto di accesso e ispezione previsto per i clienti di servizi cloud.

20) ALLINEAMENTO DELLA GESTIONE DELLA SICUREZZA PER RETI VIRTUALI E FISICHE (Rif. 13.1.3, CLD 13.1.4 ISO 27017)

Sono definiti e formalizzati, anche a livello contrattuale, lo schema delle reti e i criteri di sicurezza adottati per garantire la segregazione e la protezione tra le reti esposte su rete pubblica afferenti ai clienti e le reti interne utilizzate per l'erogazione del servizio.